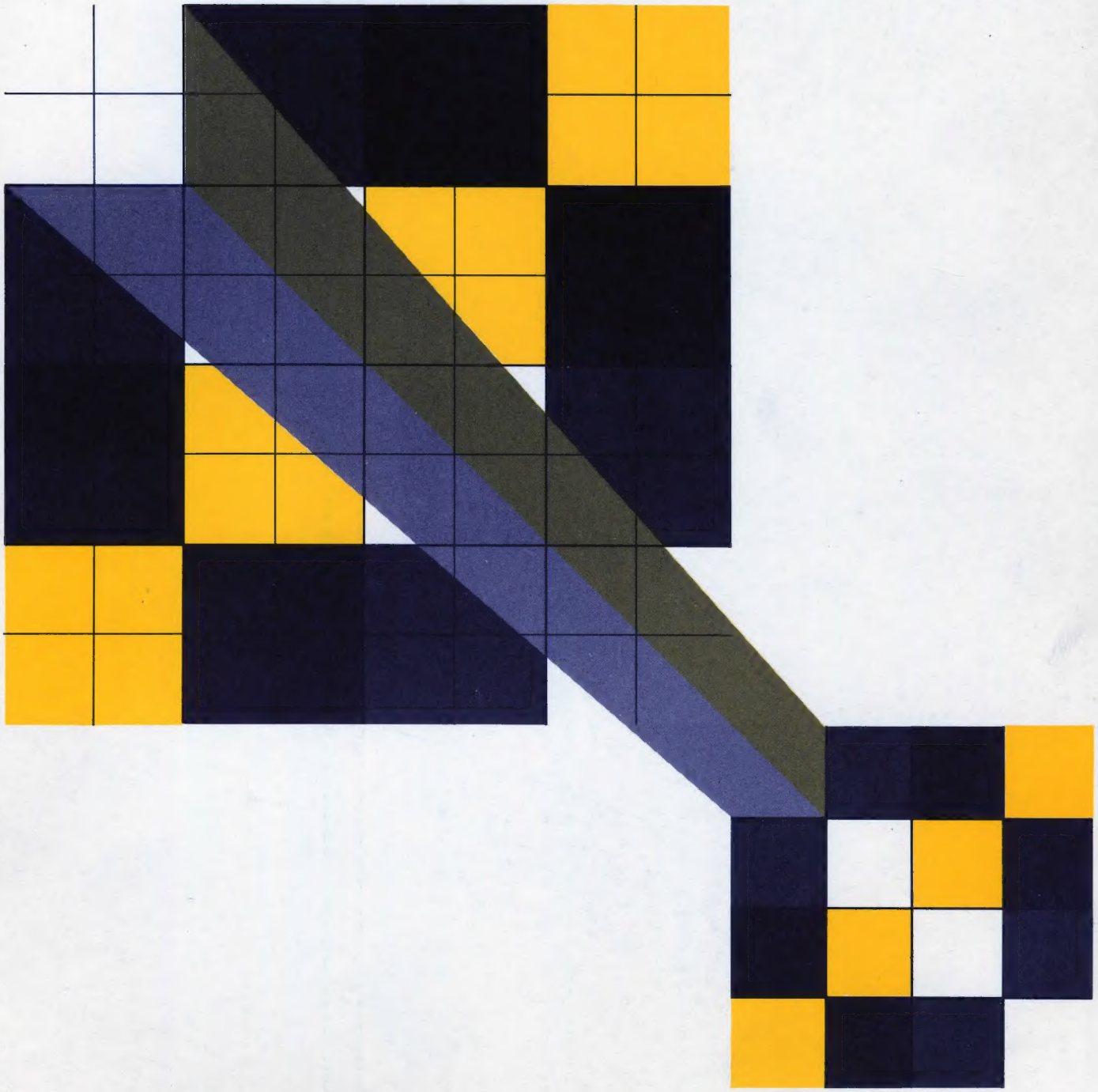
M 100 33

THE OPEN UNIVERSITY

Mathematics Foundation Course Unit 33

Groups II



The Open University

Mathematics Foundation Course Unit 33

GROUPS II

Prepared by the Mathematics Foundation Course Team

Correspondence Text 33

The Open University Press

Open University courses provide a method of study for independent learners through an integrated teaching system including textual material, radio and television programmes and short residential courses. This text is one of a series that make up the correspondence element of the Mathematics Foundation Course.

The Open University's courses represent a new system of university level education. Much of the teaching material is still in a developmental stage. Courses and course materials are, therefore, kept continually under revision. It is intended to issue regular up-dating notes as and when the need arises, and new editions will be brought out when necessary.

Further information on Open University courses may be obtained from The Admissions Office, The Open University, P.O. Box 48, Bletchley, Buckinghamshire.

The Open University Press
Walton Hall, Bletchley, Bucks

First Published 1971

Printed in Great Britain by
J W Arrowsmith Ltd, Bristol 3

SBN 335 01032 6

Contents

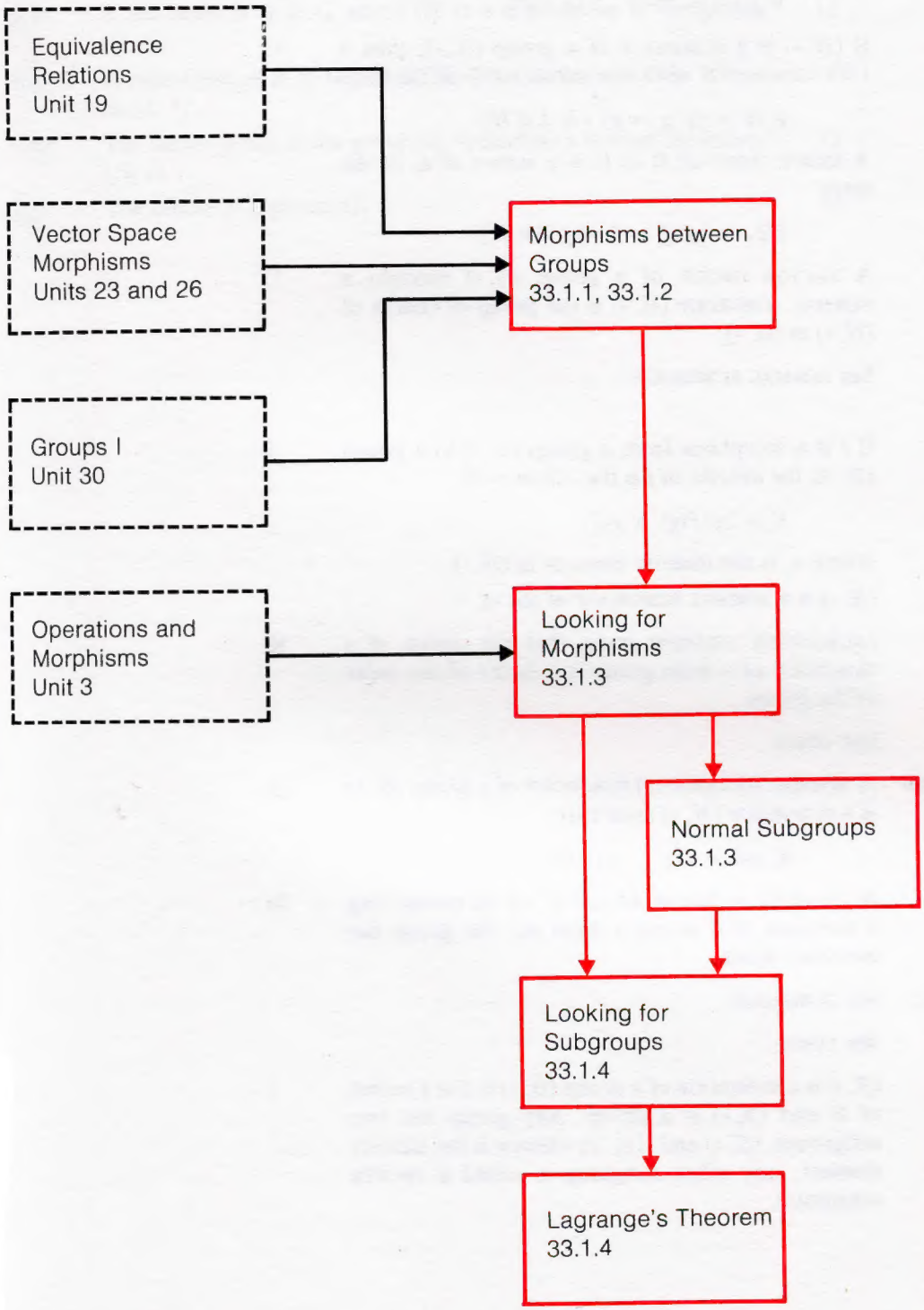
Objectives

After working through this unit you should be able to:

(i) explain the meanings of the following terms:
subgroup,
left and right cosets,
morphism from one group to another,
kernel of a morphism,
normal subgroup,
factor group,
centre of a group;
(ii) express a group as a union of cosets;
(iii) state and use the condition for a subgroup of a group to be the kernel of a morphism;
(iv) state Lagrange's theorem and use it in simple applications.

Note
Before working through this correspondence text, make sure you have read the general introduction to the mathematics course in the Study Guide, as this explains the philosophy underlying the whole course. You should also be familiar with the section which explains how a text is constructed and the meanings attached to the stars and other symbols in the margin, as this will help you to find your way through the text.

Structural Diagram



Glossary

Terms which are defined in this glossary are printed in CAPITALS.

Notation

The symbols are presented in the order in which they appear in the text.

		Page
e_g	The identity element of the group $(G, \circ)$.	7
K	The kernel of a morphism.	9
$\underline{v}$	An element of a vector space.	11
g_1H	A left coset of H in G, where $(H, \circ)$ is a subgroup of the group $(G, \circ)$.	12
Hg_1	A right coset of H in G, where $(H, \circ)$ is a subgroup of the group $(G, \circ)$.	13
G/H	The factor group of the group $(G, \circ)$ modulo a normal subgroup $(H, \circ)$.	23
Z_G	The centre of a group $(G, \circ)$.	25

Bibliography

F. Loonstra, *Introduction to Algebra* (McGraw-Hill, 1961).

The material of this unit is covered in Chapter 4; morphisms, subgroups, cosets and normal subgroups, are covered in sections 4.7, 4.8, 4.9 respectively. This book offers a more formal approach than ours, which may be of interest to those students who would like to see how the material in this unit is developed in group theory.

F. M. Hall, *An Introduction to Abstract Algebra*, Vol. 2 (Cambridge University Press, 1969).

Subgroups, cosets and Lagrange's theorem are discussed in Chapter 1; homomorphisms are discussed in Chapter 2; normal (invariant) subgroups, quotient groups and the centre of a group are discussed in Chapter 6.

33.0 INTRODUCTION

33.0

Introduction
* *

We introduced the concept of a *group* in *Unit 30* by considering symmetry in the world around us. We began by considering the set of symmetry operations on a given object (the set of mappings under which the object is invariant) and the corresponding symmetry table (showing how each pair of symmetry operations are combined under the usual law of composition to give a symmetry operation in the set). This led us to abstract the general notion of a set together with a binary operation defined on it, which satisfies four particular properties. Just to remind you, we repeat the group axioms here.

We define a group $(G, \circ)$ to be a set G with a binary operation $\circ$ defined on it, with the following properties:

(i) $\circ$ is closed;
(ii) $\circ$ is associative;
(iii) there is an identity element $e \in G$ such that for all $a \in G$

$$a \circ e = a = e \circ a;$$

(iv) for each element $a \in G$, there is an inverse element $a^{-1} \in G$ such that

$$a \circ a^{-1} = e.$$

We showed that the identity element is *unique* and that each element has a *unique* inverse.

We have seen many examples of groups in this course: groups of real numbers, complex numbers, matrices, geometric vectors, etc. In particular, $(V, +)$ is a group, where V is a vector space (see the vector space axioms 1, 2, 4 and 6, given in *Unit 22*, section 22.2.2). We define a *subgroup* of a group by analogy with our definition of a vector subspace: $(S, \circ)$ is a subgroup of $(G, \circ)$ if S is a subset of G such that $(S, \circ)$ is itself a group. Any group $(G, \circ)$ has two subgroups, $(G, \circ)$ and $(\{e\}, \circ)$, where e is the identity element; any other subgroup is called a proper subgroup.

Definition 1
* * *

In this unit we aim to give you a general impression of what mathematicians call *group theory*. We do this by proving two very general theorems, which together with Cayley's theorem (which you met in *Unit 30, Groups I*) are a basis for group theory.

The first of the two major theorems is a theorem about any group. It gives, in theory, a method for determining all the morphisms which have a given group as their domain.

The second theorem is a very powerful theorem due to Lagrange which applies to all groups with a finite number of elements. It states that, if $(H, \circ)$ is a subgroup of a finite group $(G, \circ)$, then the number of elements in H is a factor of the number of elements in G. The power of this theorem lies in the fact that to find all the proper subgroups of a group of 10 elements, say, we do not need to consider *all* the possible subsets of a set of 10 elements, but we need only consider the subsets containing 2 or 5 elements.

This unit is considerably shorter than most units in this course, but the individual statements often require considerable concentration. The type of mathematical argument given in this text is very important. It is typical of much mathematical thinking today, and is very different from the "find a solution of the following equation" type of argument.

33.1 MORPHISMS AND SUBGROUPS

33.1

33.1.1 Morphisms between Groups

33.1.1

Discussion
* *

One feature of *Unit 30, Groups I* was the fact that effectively the same group tables kept cropping up in different contexts. This feature was characterized by Cayley's theorem which tells us that *every* group can be considered as a group of permutations.

For example, the group of all permutations of three objects is essentially the same as the symmetry group of the equilateral triangle. A particular subgroup of the group of all permutations of four objects is essentially the same as the symmetry group of the rectangle, which is in turn essentially the same as the symmetry group of the water molecule. By *essentially the same* we mean that the groups differ only in their physical origins, in the group operation, and in the labels we happen to choose for the group elements. Thus we are able to say that the table

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

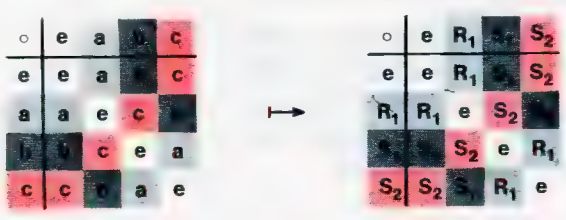
defines the Klein 4-group. By a suitable one-one mapping, we can map the table for the symmetry group of the water molecule to this table. We can do the same with the symmetry group of the rectangle. For example, in *Unit 30* we met the symmetry group of the rectangle in the form

$\circ$	e	R_1	S_1	S_2
e	e	R_1	S_1	S_2
R_1	R_1	e	S_2	S_1
S_1	S_1	S_2	e	R_1
S_2	S_2	S_1	R_1	e

and the mapping

$$e \longmapsto e$$
$$a \longmapsto R_1$$
$$b \longmapsto S_1$$
$$c \longmapsto S_2$$

maps the first table to the second. The mapping not only maps the set $\{e, a, b, c\}$ to the set $\{e, R_1, S_1, S_2\}$ but it preserves the structure of the table.



This mapping is an isomorphism. The name "Klein 4-group" is the name of an abstract group which is used as a model for any group which is isomorphic to it. In studying the Klein 4-group we study at the same time any isomorphic group, and any situation represented by such a group.

So in the context of groups isomorphisms enable us to talk of an abstract group and (as always with isomorphisms) to establish links between apparently different situations. Practically, isomorphisms offer us no simplification; what they do offer is an economy of effort and a choice of situation in which to work.

On the other hand, homomorphisms offer us a chance of simplification. Because a homomorphism is a many-one mapping, we may be able to deal with a set of, say, four objects instead of twelve. Of course, there is always a price to pay for simplification — some of the detail is lost — but because we have a morphism we do still hang on to the structure. Homomorphisms can help us to get an idea of the wood without inspecting all the trees.

A case in point is the example we use in the television programme for this unit. By separating the elements of the symmetry group of the triangle into two classes — reflections (the S's) and rotations (the R's), we can map the group table

	e	R_1	R_2	S_1	S_2	S_3
e	e	R_1	R_2	S_1	S_2	S_3
R_1	R_1	R_2	e	S_3	S_1	S_2
R_2	R_2	e	R_1	S_2	S_3	S_1
S_1	S_1	S_2	S_3	e	R_1	R_2
S_2	S_2	S_3	S_1	R_2	e	R_1
S_3	S_3	S_1	S_2	R_1	R_2	e

to the group table

□	0	1
0	0	1
1	1	0

Although we lose information about how individual elements combine, the overall pattern of the group is given emphasis — for example, the fact that any two reflections in this particular group always combine to give a rotation.

Exercise 1

Exercise 1
(5 minutes)

(i) From *Unit 23*, section 23.2.4, we know that the matrix

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

represents a rotation of the plane through an angle θ clockwise about the origin. Taking $\theta = 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$, we obtain the matrices

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathscr{R}_1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

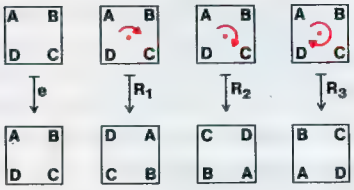
$$\mathscr{R}_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathscr{R}_3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

respectively.

The set $\{E, \mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3\}$ is a group for the operation of matrix multiplication. Write down the table for this group.

(ii) The set of complex numbers $\{1, -i, -1, i\}$ is a group for multiplication. Write down the table for this group.

(iii) Compare the tables in (i) and (ii) with the table for the rotational group of the square:



$\circ$	e	R_1	R_2	R_3
e	e	R_1	R_2	R_3
R_1	R_1	R_2	R_3	e
R_2	R_2	R_3	e	R_1
R_3	R_3	e	R_1	R_2

■

Discussion

As an example of a group homomorphism, consider the set of integers Z under addition. The set Z can be mapped to the set $S = \{a, b\}$ as follows:

$$n \longmapsto a, \text{ if } n \text{ is odd}$$
$$n \longmapsto b, \text{ if } n \text{ is even} \qquad (n \in Z)$$

(zero is considered to be even).

The mapping is a homomorphism from $(Z, +)$ to $(S, \square)$ for the operation $\square$ on $\{a, b\}$ defined by the table

$\square$	a	b
a	b	a
b	a	b

This table tells us something about addition on the set of integers. It tells us that the equivalence class O of odd integers and the equivalence class E of even integers combine in a certain way; we can talk of "addition of the equivalence classes" defined by the table

$\square$	O	E
O	E	O
E	O	E

(See *Unit 19*, Exercise 19.2.3.1.)

Of course, this example is in a sense too familiar to seem of any value. We know that

$$Odd + Odd = Even$$

and so on; in fact that is how we knew that we had a morphism. But suppose we had very little knowledge about the integers under addition. The existence of a morphism would give us an idea how the integers behaved "in the large". An isomorphism reflects the fine detail of element by element behaviour: the homomorphism tells us something about the "coarse" structure of the integers.

Exercise 2

Exercise 2
(2 minutes)

Show that the set $\{a, b\}$ with operation $\square$ as defined by the table in the text is a group. ■

Discussion
* *

Exercise 2 should come as no surprise. We know that a homomorphism preserves structure; so if the domain is a group we expect that the image set will also be a group for the appropriate operation. (We have seen another example of the same sort of thing in *Unit 23, Linear Algebra II*. There we showed that the image of a vector space under a morphism is again a vector space.) We have the following formal statement:

THEOREM

Theorem
* * *

If f is a morphism from the group $(G, \circ)$ to $(H, \square)$ and $f(G) = H$, then $(H, \square)$ is a group.

(The proof of this theorem is rather tedious. You can safely ignore it if you are short of time.)

PROOF

We have to verify the four group properties:
(i) closure
(ii) associativity
(iii) identity element
(iv) inverses
for $(H, \square)$, using two pieces of information:
(1) $(G, \circ)$ satisfies the group axioms;
(2) f is a morphism.

(i) *Closure*

We need to prove that if h_1, h_2 are any elements of H, then $h_1 \square h_2 \in H$.

If $h_1, h_2 \in H$, then, since $f(G) = H$, there are elements g_1 and g_2 in G such that

$$f(g_1) = h_1,$$
$$f(g_2) = h_2.$$

Then

$$h_1 \square h_2 = f(g_1) \square f(g_2)$$
$$= f(g_1 \circ g_2) \qquad (f \text{ is a morphism}),$$

and $g_1 \circ g_2 \in G$ because $(G, \circ)$ is closed. Since $f(G) = H$, $f(g_1 \circ g_2)$ must belong to H, i.e. $h_1 \square h_2 \in H$, and so $(H, \square)$ is closed.

(ii) *Associativity*

We need to show that for any $h_1, h_2, h_3 \in H$,

$$h_1 \square (h_2 \square h_3) = (h_1 \square h_2) \square h_3.$$

Suppose h_1, h_2, $h_3 \in H$ and that $f(g_1) = h_1$, $f(g_2) = h_2$ and $f(g_3) = h_3$.

The operation $\circ$ is associative, and so

$$g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$$

But

$$f(g_1 \circ (g_2 \circ g_3)) = f(g_1) \square f(g_2 \circ g_3)$$
$$= f(g_1) \square (f(g_2) \square f(g_3))$$
$$= h_1 \square (h_2 \square h_3),$$

(*continued on page 7*)

Solution 1

Solution 1

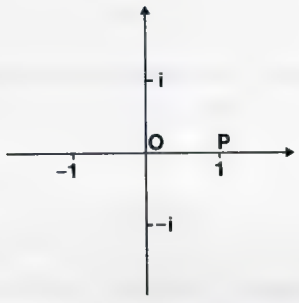
(i) The table for the matrix group is the same as that for the rotational group of the square. This is not surprising, because the matrices $E, \mathscr{R}_1, \mathscr{R}_2, \mathscr{R}_3$ correspond to clockwise rotations of the plane through $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ respectively.

(ii) The table is

$\times$	1	$-i$	-1	i
1	1	$-i$	-1	i
$-i$	$-i$	-1	i	1
-1	-1	i	1	$-i$
i	i	1	$-i$	-1

If we replace $1, -i, -1, i$ by e, R_1, R_2, R_3 respectively, and replace $\times$ by $\circ$, we obtain the table given in (iii).

Again, this is not surprising.



Multiplying the number 1 by $1, -i, -1, i$ has the effect of rotating the geometric vector $\overrightarrow{OP}$ clockwise about the origin through $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ respectively.

(iii) All three groups have the same structure: the group tables are essentially the same. ■

Solution 2

Solution 2

From the table we see that b is an identity element, each element is its own inverse and the set is closed, because only a's and b's appear in the table. Associativity can be checked by looking at all possible combinations, e.g., $a \square (b \square a)$, $(a \square b) \square a$, etc., or by recognizing that the operation $\square$ is essentially $\oplus_2$, which is associative. ■

(*continued from page 5*)

and, similarly,

$$f((g_1 \circ g_2) \circ g_3) = (h_1 \square h_2) \square h_3$$

Thus

$$h_1 \square (h_2 \square h_3) = (h_1 \square h_2) \square h_3,$$

and since there was no restriction on the choice of g_1, g_2 and g_3, this equation holds for all h_1, h_2 and h_3 in H.

(iii) *Identity Element*

We need to show that there is an element $e_h \in H$, such that

$$e_h \square h = h \square e_h = h,$$

where h is *any* element of H.

Let $h \in H$; then there is an element $g \in G$, such that $f(g) = h$.

If e_g is the identity in G, then

$$e_g \circ g = g \circ e_g = g.$$

It follows that

$$f(e_g \circ g) = f(g \circ e_g) = f(g)$$

and thus,

$$f(e_g) \square f(g) = f(g) \square f(e_g) = f(g).$$

If

$$f(e_g) = e_h,$$

then

$$e_h \square h = h \square e_h = h,$$

which shows that H has an identity element, e_h.

(iv) *Inverses*

We need to show that for any $h \in H$ there is an element $h^{-1} \in H$ such that

$$h \square h^{-1} = e_h.$$

If h is any element of H and $f(g) = h$, then there is an element $g^{-1} \in G$ such that

$$g \circ g^{-1} = e_g.$$

It follows that

$$f(g \circ g^{-1}) = f(g) \square f(g^{-1}) = f(e_g) = e_h \qquad \text{(by (iii))}$$

i.e. an inverse of h is $h^{-1} = f(g^{-1})$.

Hence $(H, \square)$ is a group.

In *Unit 30*, section 30.2.5, we showed that a group has a *unique* identity element, and that each element of a group has a *unique* inverse. Hence, under the morphism

$$f: (G, \circ) \longmapsto (H, \square),$$

we have

(i) $f(e_g) = e_h,$

i.e. the identity element in $(G, \circ)$ is mapped to the identity element in $(H, \square)$;

(ii) if

$$f(g) = h,$$

then h has the unique inverse

$$h^{-1} = f(g^{-1})$$

i.e. the inverse element of the image of g is the image of the inverse element of g.

Exercise 3

Exercise 3
(10 minutes)

In each of the following cases say whether or not the two groups defined by the tables are isomorphic. If you think a pair are isomorphic, describe the re-labelling of the elements which specifies the isomorphism. If you think a pair are not isomorphic, give a reason.

(i)

∘	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(a)

□	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(b)

(ii)

∘	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(a)

□	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(b)

(iii)

∘	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

(a)

□	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

(b) ■

33.1.2 Some More Results Suggested by Linear Algebra

33.1.2

Main Text
* *

The image of a vector space under a morphism is a vector space.

The image of a group under a morphism is a group.

The first result we found in *Unit 23, Linear Algebra II*; the second we have just found. What other results from morphisms in linear algebra can we carry over to morphisms in groups?

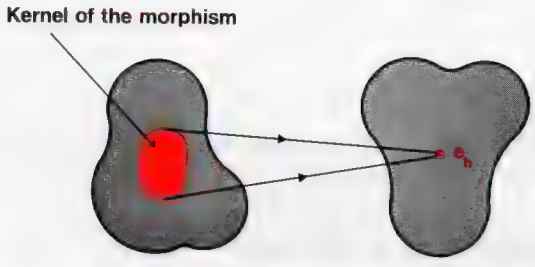
One of the fundamental ideas connected with a morphism in linear algebra is the kernel: the set of elements in the domain of a morphism which are mapped to the zero element in the codomain. (See *Unit 23*, section 23.1.3.) Let us look at this idea from the group point of view. The elements of a vector space under addition form a group, and the zero element of the vector space is the identity element of this group. So we define the kernel of a group morphism as follows.

If f is a morphism from a group $(G, \circ)$ to a group $(H, \square)$, and if e_h is the identity element in H, then the set

$$\{g : g \in G, f(g) = e_h\}$$

is called the kernel of the morphism.

Definition 1
* * *



The first thing we proved about the kernel of a vector space morphism was that it is itself a vector space. We suspect immediately that the kernel of a group morphism gives a group, that is, $(K, \circ)$ is a subgroup of $(G, \circ)$. We ask you to prove this in the following exercise.

Exercise 1

Exercise 1
(4 minutes)

Fill in the empty boxes to complete the following proof that the kernel of the morphism $f:(G, \circ) \longmapsto (H, \square)$ is a subgroup of $(G, \circ)$.

Let K be the kernel of f.

(i) *Closure*

If $g_1, g_2 \in K$, then

$$f(g_1) = f(g_2) = \boxed{} \qquad \text{(a)}$$

and, using the fact that f is a morphism, we have

$$f(g_1 \circ g_2) = \boxed{} \qquad \text{(b)}$$

$$= \boxed{} \qquad \text{(c)}$$

and so

$$g_1 \circ g_2 \in K.$$

(*continued on page 11*)

Solution 33.1.1.3 **Solution 33.1.1.3**

(i) If we re-label table (a) as follows,

$1 \longmapsto 0$

$2 \longmapsto 3$

$3 \longmapsto 1$

$4 \longmapsto 2$

we get

$\circ$	0	3	1	2
0	0	3	1	2
3	3	2	0	1
1	1	0	2	3
2	2	1	3	0

and rearranging rows and columns, and writing $\square$ instead of $\circ$, gives

$\square$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

which is the same table as table (b) in the question. Thus the mapping above is an isomorphism. A partial chain of reasoning to arrive at the mapping is as follows.

1 It is clear from the first row and the first column of each table that, in (a), 1 is the identity, and, in (b), 0 is the identity. Thus we want to map 1 to 0.

2 In (a) $4 \circ 4 = 1$ and in (b) the only element (other than the identity) which combines with itself to give the identity is 2; $2 \square 2 = 0$. Thus we want to map 4 to 2.

3 This leaves 2 and 3 in table (a) and 1 and 3 in table (b) to deal with. Mapping 2 to 3 and 3 to 1 establishes the isomorphism. (We could also have mapped 2 to 1 and 3 to 3 and obtained a different isomorphism.)

(ii) In each of the tables, a is the identity. In table (b) every element is its own inverse: this is shown by the fact that every element in the "top left to bottom right" diagonal is the identity. This is not the case in table (a) — for example, $b \circ b$ is not the identity. So we cannot map b to any of a, b, c and d.

(iii) Again, the groups represented by these tables are not isomorphic. In each case, e is the identity, and in table (a) three elements beside e are their own inverses. But in table (b) only one other element is its own inverse. ■

(ii) ***Associativity***

(*continued from page 9*)

$\circ$ in K is associative because $\square$ (d)

(iii) ***Identity Element***

$e_g \in K$ because $f(e_g) = \square$ (e)

(iv) ***Inverses***

If $g \in K$, then $g^{-1} \in K$ because

$$f(g \circ g^{-1}) = f(e_g) = \square \quad \text{(f)}$$

and, using the fact that f is a morphism, we have

$$f(g \circ g^{-1}) = \square \quad \text{(g)}$$

$$= \square \ \square \ f(g^{-1}) \quad \text{(h)}$$

$$= \square \quad \text{(i)}$$

and, comparing (f) and (i), we have

$$f(g^{-1}) = \square \quad \text{(j)}$$

and thus

$$g^{-1} \in K. \quad \blacksquare$$

Discussion
* *

Looking again at *Unit 23*, section 23.1.3, we find that the next result we mentioned was the so-called "dimension theorem". We defined the dimension of a vector space to be the maximum number of linearly independent vectors in the space. Have we an analogue of dimension for a general group?

For a general group we have no set of scalars with which to define a linear combination of elements: so the ideas of linear independence and dimension are not obviously applicable to groups. (In fact, these ideas *are* applicable to Abelian groups — but that's another story.)

So let us look on to the next section in *Unit 23*, section 23.1.4. There we proved the following result:

If L is a morphism from a vector space V to a vector space U and K is its kernel, then the set of all elements which map to a given element $\underline{u} \in U$ can be written in the form

$$\{\underline{v} : \underline{v} = \underline{v}_1 + \underline{k}, \underline{k} \in K\}, \text{ where } L(\underline{v}_1) = \underline{u}.$$

That is, the set of all elements which map to $\underline{u}$ can be obtained by adding one element which maps to $\underline{u}$, $\underline{v}_1$ say, to each of the elements of the kernel.

This result was important in *Unit 26*, *Linear Algebra III* when we considered the solution of systems of simultaneous equations. In particular, it led to one interesting conclusion: if the number of elements in the kernel is finite, say n, then there are exactly n elements in the domain which map to *any* given element in the image set. Can we adapt this result to groups?

(*continued on page 12*)

Solution 1

Solution 1

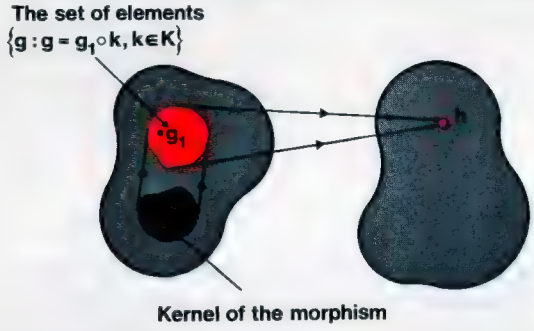
(i) (a) e_h, (b) $f(g_1) \square f(g_2)$, (c) e_h.
(ii) (d) $(G, \circ)$ is a group.
(iii) (e) e_h.
(iv) (f) e_h, (g) $f(g) \square f(g^{-1})$, (h) e_h, (i) $f(g^{-1})$, (j) e_h. ■

(continued from page 11)

There does not appear to be any reason why not. We can easily rewrite the result in terms of groups:

If f is a morphism from a group $(G, \circ)$ to a group $(H, \square)$ and K is its kernel, then the set of all elements which map to a given element $h \in H$ can be written in the form

$$\{g : g = g_1 \circ k, k \in K\}, \text{ where } f(g_1) = h.$$



We ask you to prove this result in the next exercise.

Exercise 2

Exercise 2
(4 minutes)

With the notation as in the statement above, show that
(i) $f(g_1 \circ k) = h \qquad (k \in K)$;
(ii) if

$$f(g_1) = f(g_2) = h,$$

then

$$g_2 = g_1 \circ k$$

for some $k \in K$.
(HINT: Consider $f(g_1^{-1} \circ g_2)$.)
These two results together prove the statement in the text. ■

Exercise 3

Exercise 3
(2 minutes)

In a vector space the operation $+$ is commutative, but in a group $(G, \circ)$ the operation $\circ$ is not necessarily commutative. So we could have generalized the vector space statement to obtain a second set

$$\{g : g = k \circ g_1, \quad k \in K\}.$$

Show that this set of elements is the same as the set

$$\{g : g = g_1 \circ k, \quad k \in K\}.$$ ■

In order to save ourselves writing

Main Text ★★

$$\{g : g = g_1 \circ k, k \in K\},$$

we give such a set the label g_1K and call it a left coset of K in G, because g_1

Definitions 2 ★★★

stands on the left. Similarly, we write

$$Kg_1 = \{g : g = k \circ g_1, k \in K\}$$

and call it a right coset of K in G.

Can we now conclude that if the number of elements in the kernel is finite, say n, then there are exactly n elements in G which map to any element in H? We need to show that

$$k_1 \neq k_2 \Rightarrow g_1 \circ k_1 \neq g_1 \circ k_2.$$

We can prove this easily by contradiction. Suppose $k_1 \neq k_2$ and

$$g_1 \circ k_1 = g_1 \circ k_2.$$

Then g_1^{-1} exists, and so

$$g_1^{-1} \circ (g_1 \circ k_1) = g_1^{-1} \circ (g_1 \circ k_2)$$

i.e.

$$(g_1^{-1} \circ g_1) \circ k_1 = (g_1^{-1} \circ g_1) \circ k_2$$

or

$$k_1 = k_2,$$

which contradicts our hypothesis. So the elements of g_1K are all different, and similarly for Kg_1. If there are n distinct elements in K, then g_1K and Kg_1 each have n distinct elements.

Exercise 4

Exercise 4
(3 minutes)

In each of the following cases, describe the kernel K of the morphism and the left cosets of the kernel.

(i) The set of non-zero complex numbers C_1 under multiplication is a group, and

$$z \longmapsto z^n \quad (z \in C_1),$$

where n is a positive integer, is a morphism from $(C_1, \times)$ to $(C_1, \times)$.

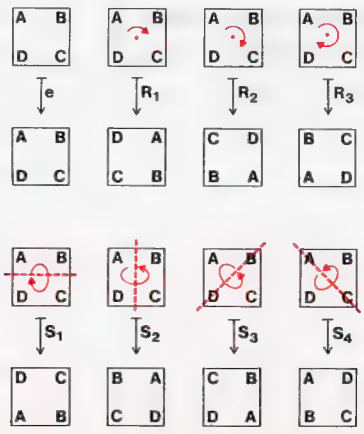
(ii) The set of 2×2 matrices, M_2, under addition is a group, and if A is any 2×2 matrix, then

$$X \longmapsto AX \qquad (X \in M_2)$$

is a morphism from $(M_2, +)$ to a subset of itself. We choose two particular cases:

(a) $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ (b) $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.

(iii) The symmetry group of the square has eight elements as shown in the figure.



(*continued on page 14*)

Solution 2 **Solution 2**

(i) $f(g_1 \circ k) = f(g_1) \square f(k) = h \square e_h = h.$

(ii) $f(g_1^{-1} \circ g_2) = f(g_1^{-1}) \square f(g_2)$

$= h^{-1} \square h \qquad ((f(g_1))^{-1} = f(g_1^{-1}))$

$= e_h.$

So $g_1^{-1} \circ g_2 \in K$, i.e.

$$g_1^{-1} \circ g_2 = k$$

for some $k \in K$. Whence

$g_1 \circ (g_1^{-1} \circ g_2) = g_1 \circ k$

i.e.

$$g_2 = g_1 \circ k. \qquad \blacksquare$$

Solution 3 **Solution 3**

The sets of elements are the same: we can go through the two parts of the proof as in Exercise 2, except that in (ii) we start with $f(g_2 \circ g_1^{-1})$. Notice that it is not sufficient to show that $g = k \circ g_1$ has image h and so belongs to the first set. This only shows that the second set is a subset of the first set. ■

(*continued from page 13*)

The group table is

$\circ$	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
e	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
R_1	R_1	R_2	R_3	e	S_4	S_3	S_1	S_2
R_2	R_2	R_3	e	R_1	S_2	S_1	S_4	S_3
R_3	R_3	e	R_1	R_2	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	e	R_2	R_1	R_3
S_2	S_2	S_4	S_1	S_3	R_2	e	R_3	R_1
S_3	S_3	S_2	S_4	S_1	R_3	R_1	e	R_2
S_4	S_4	S_1	S_3	S_2	R_1	R_3	R_2	e

The rotations e, R_1, R_2, R_3 do not turn the square over, whereas the reflections S_1, S_2, S_3, S_4 turn the square over. If we denote turning the square over by T, and not turning it over by N, then we have the following fairly obvious combination table for N and T.

$\square$	N	T
N	N	T
T	T	N

The mapping which maps e, R_1, R_2, R_3 to N and S_1, S_2, S_3, S_4 to T, is a morphism for the obvious operations. ■

Summary

Summary

Let f be a morphism from a group $(G, \circ)$ to a group $(H, \square)$.

(1) The kernel K of f is the set

$$\{g : g \in G, f(g) = e_h\},$$

where e_h is the identity in H.

(2) $(K, \circ)$ is a subgroup of $(G, \circ)$.

(3) A left coset of K in G is a subset of G of the form

$$g_1K = \{g : g = g_1 \circ k, k \in K\}.$$

(4) $f(g_1 \circ k) = f(g_1)$, where k is any element of K; i.e. the image of every element in a left coset of K is the same. Further, g_1K contains *all* the elements of G with image $f(g_1)$.

(5) We have similar results for right cosets, denoted by Kg_1, and, in particular,

$$g_1K = Kg_1.$$

We proved this result in Exercise 3. Note that we have shown that the two *sets* are equal: this does NOT mean that

$$\forall_k \quad g_1 \circ k = k \circ g_1 \qquad (k \in K).$$

Discussion

Note that left and right cosets of H in G are defined where $(H, \circ)$ is *any* subgroup of $(G, \circ)$, not necessarily the kernel of a morphism; but in this case corresponding left and right cosets are not necessarily equal.

All these results and terms were suggested by results and terms previously encountered in linear algebra. In *Unit 23* we also discussed various ways of combining morphisms. We shall not discuss this in this unit; we feel that the next section, in which we shall look at a point not discussed in *Unit 23*, leads to more important results for inclusion in a short introduction to group theory.

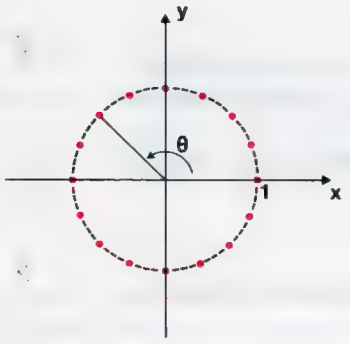
Solution 4

Solution 4

(i) $K = \{z : z^n = 1\}$

$= \{e^{i(2m\pi/n)} : m = 0, 1, \ldots, n-1\}.$

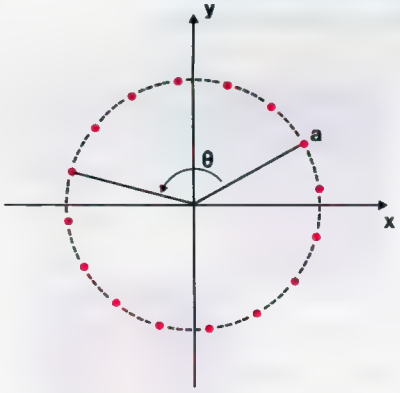
This set, for the case $n = 16$, is represented by the red dots in the following diagram. The angle θ is the Argument of the element of K for which $m = 6$.



The left coset of K for a general element $a \in C$ is

$$aK = \{a \times e^{i(2m\pi/n)} : m = 0, 1, 2, \ldots, n-1\}.$$

This set, for the case $n = 16$, θ as above, is represented by the red dots in the following diagram.



(ii) $K = \{X : AX = O\}$

Let

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(a) $$AX = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ c-a & d-b \end{pmatrix}.$$

If

$AX = O,$

then

$$X = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \qquad a, b \in R.$$

So

$$K = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} : a, b \in R \right\}$$

The left cosets of K for $B \in M_2$ are each of the form

$$BK = \left\{ B + \begin{pmatrix} a & b \\ a & b \end{pmatrix} : a, b \in R \right\}$$

(b)
$$AX = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c - a & d - b \end{pmatrix}$$

If

$$AX = O,$$

then

$$X = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

so

$$K = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

The left cosets of K for $C \in M_2$ are each of the form $\{C\}$.

(iii) $K = \{e, R_1, R_2, R_3\}$, since the identity in the image set is N.

There are only two left cosets, K itself and $\{S_1, S_2, S_3, S_4\}$. ■

33.1.3 Looking for Morphisms

33.1.3

Main Text
* *

One thing which we did not do in *Unit 23, Linear Algebra II* was to look for morphisms: they were all obvious and could be characterized very simply. The trouble with group morphisms is that they are not always obvious, except perhaps when we know something about the physical meaning of the group. For instance, if we have a symmetry group, we can fairly easily find some morphisms geometrically. This is effectively what we did in Exercise 33.1.2.4 (iii), with the symmetry group of the square. We shall not give any theoretical justification of this, because it does not solve the problem for any abstract group. Instead we shall go almost right back to the beginning of the course.

We first started looking for morphisms in *Unit 3, Operations and Morphisms*, and we pointed out there that the usual situation is one in which we have a set A with a binary operation $\circ$, and a function f mapping A to $f(A)$. Our problem then in looking for a morphism was to look for a binary operation $\square$ on $f(A)$ such that

$$f(a_1) \square f(a_2) = f(a_1 \circ a_2),$$

for all $a_1, a_2 \in A$. We found that sometimes there was such an operation $\square$ and sometimes there wasn't, and we established a criterion for the existence of $\square$: the compatibility of f with $\circ$. To remind you, compatibility was defined as follows.

A function f with domain A and a binary operation $\circ$ on A are compatible if whenever

$$f(a_1) = f(a_2), \qquad a_1, a_2 \in A,$$

and

$$f(a_3) = f(a_4), \qquad a_3, a_4 \in A,$$

then

$$f(a_1 \circ a_3) = f(a_2 \circ a_4).$$

So our group problem is also solved in the sense that, given a group $(G, \circ)$ and a function f, we can test whether f and $\circ$ are compatible: if they are, then f is a morphism of $(G, \circ)$ to $(f(G), \square)$ where $\square$ is defined by

$$f(g_1) \square f(g_2) = f(g_1 \circ g_2).$$

This, however, is not very satisfactory. We already know quite a bit about a group morphism. For instance, it has a kernel K such that $(K, \circ)$ is a subgroup of the original group. And we are not using any of this information. A group is a very particular sort of mathematical animal and we should suspect that the general idea of compatibility for *any* set A with a binary operation $\circ$ can be modified for a group G with its *particular* binary operation $\circ$. So we shall now look at the definition of compatibility again, bearing in mind that we are dealing with a group $(G, \circ)$.

Let f be a morphism from $(G, \circ)$ to $(f(G), \square)$; then f and $\circ$ are compatible. This means that whenever

$$f(g_1) = f(g_2), \qquad g_1, g_2 \in G,$$

and

$$f(g_3) = f(g_4), \qquad g_3, g_4 \in G,$$

then

$$f(g_1 \circ g_3) = f(g_2 \circ g_4).$$

Now look at the Summary of section 33.1.2 and remember that all the results there are a necessary consequence of f being a morphism. We shall now show that they are also sufficient for f to be a morphism; i.e. that we can prove compatibility of f and $\circ$ from them.

In part (4) of the Summary we have

g_1K contains all the elements of G with image $f(g_1)$,

and in part (5) we have

$$g_1K = Kg_1.$$

From

$$f(g_1) = f(g_2)$$

it follows that

$$g_2 = g_1 \circ k_2$$

for some $k_2 \in K$.

Similarly, from

$$f(g_3) = f(g_4)$$

it follows that

$$g_4 = g_3 \circ k_4$$

for some $k_4 \in K$.

Hence

$$f(g_2 \circ g_4) = f(g_1 \circ k_2 \circ g_3 \circ k_4)$$

(We omit the brackets in $g_1 \circ k_2 \circ g_3 \circ k_4$: we take associativity for granted.)

Now we use part (5) to write

$$k_2 \circ g_3 = g_3 \circ k_3$$

for some $k_3 \in K$, so that

$$f(g_2 \circ g_4) = f(g_1 \circ g_3 \circ k_3 \circ k_4)$$

But $(K, \circ)$ is a subgroup (part (2) of the Summary), so

$$k_3 \circ k_4 = k_1$$

for some $k_1 \in K$.

That is,

$$f(g_2 \circ g_4) = f(g_1 \circ g_3 \circ k_1)$$

Applying part (4) again, we have

$$f(g_1 \circ g_3) = f(g_1 \circ g_3 \circ k_1),$$

so, finally, we have

$$f(g_2 \circ g_4) = f(g_1 \circ g_3).$$

We have proved that the five points in our Summary at the end of section 33.1.2 are both necessary and sufficient for the existence of a group morphism.

Let us look at these five points: we repeat them here for convenience.

If f is a morphism from a group $(G, \circ)$ to a group $(H, \square)$, then:

(1) the kernel K of f is the set

$$\{g : g \in G, f(g) = e_h\},$$

where e_h is the identity in H;

(2) $(K, \circ)$ is a subgroup of $(G, \circ)$;

(3) a left coset of K is a subset of G of the form

$$g_1K = \{g : g = g_1 \circ k, k \in K\};$$

(4) $f(g_1 \circ k) = f(g_1)$, where k is any element of K; i.e. the image of every element in a left coset of K is the same; further, g_1K contains *all* the elements of G with image $f(g_1)$;

(5) we have similar results for right cosets, denoted by Kg_1, and, in particular,

$$g_1K = Kg_1.$$

(1) and (3) are just definitions.

Discussion

(2) states that a morphism has a kernel K such that $(K, \circ)$ is a subgroup of the group $(G, \circ)$. So we can begin our search for the morphisms of the group $(G, \circ)$ by looking for all its subgroups.

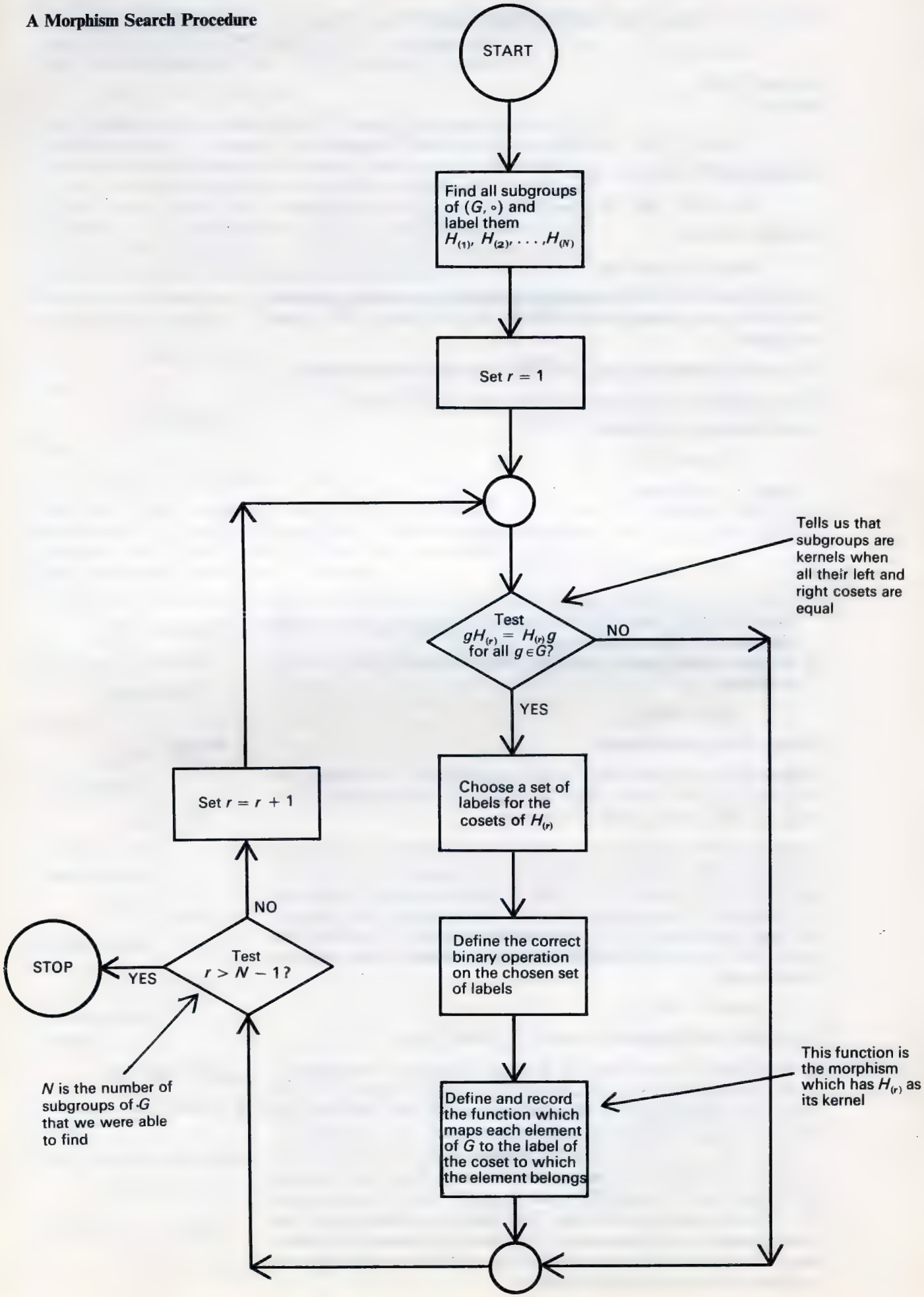
(5) tells us that if a subgroup is a kernel of some morphism, then left cosets are equal to right cosets. So we can test each subgroup we have found to see if left cosets are equal to right cosets. If they are not, then the subgroup is *not* the kernel of a morphism. If they are, then we can use (4) to construct the image set, because (4) tells us that the elements of a left coset (or right coset) of the kernel are all mapped to the same element in the image set. We shall write

$$f(g_1K) = f(g_1)$$

(i.e. we shall not distinguish between $\{f(g_1)\}$ and $f(g_1)$).

So all we have to do is invent a set of labels for the cosets and define the correct combinations on this set of labels. Then finally we define a function which maps each element of G to the label for the coset to which that element belongs. This function is the morphism with the given subgroup as kernel. Thus, we are now able to construct *all* the morphisms from a group $(G, \circ)$, directly from the group itself. We do not even have to choose a function and test for compatibility: all we need to start with is the group $(G, \circ)$. We then construct all the rest: the image set, the function, and the binary operation on the image set which turns the function into a morphism. The process (for a group with a finite number of subgroups) can be illustrated by the following diagram.

A Morphism Search Procedure



Example 1

Example 1

Let us apply this morphism search procedure to the symmetry group $(G, \circ)$ of the square whose table is given again below.

$\circ$	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
e	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
R_1	R_1	R_2	R_3	e	S_4	S_3	S_1	S_2
R_2	R_2	R_3	e	R_1	S_2	S_1	S_4	S_3
R_3	R_3	e	R_1	R_2	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	e	R_2	R_1	R_3
S_2	S_2	S_4	S_1	S_3	R_2	e	R_3	R_1
S_3	S_3	S_2	S_4	S_1	R_3	R_1	e	R_2
S_4	S_4	S_1	S_3	S_2	R_1	R_3	R_2	e

(i) The proper subgroups are $(H, \circ)$ for the following sets H:

$$\{e, R_1, R_2, R_3\}, \{e, R_2\}, \{e, S_1\}, \{e, S_2\}, \{e, S_3\}, \{e, S_4\},$$
$$\{e, R_2, S_1, S_2\}, \{e, R_2, S_3, S_4\}.$$

(In the next section we shall consider the obvious question of how we find these subgroups.)

(ii) Choose a subgroup $(H, \circ)$; we start with $H = \{e, S_4\}$. We now have to test whether $gH = Hg$, for all $g \in G$. We shall go through the group elements in order, except that we note that if $g \in H$, then

$$gH = H = Hg$$

so we do not have to test elements of H itself.

$$R_1\{e, S_4\} = \{R_1 \circ e, R_1 \circ S_4\} = \{R_1, S_2\}.$$
$$\{e, S_4\}R_1 = \{e \circ R_1, S_4 \circ R_1\} = \{R_1, S_1\}.$$

And we can stop, since for our first choice of $g = R_1$,

$$R_1H \neq HR_1.$$

(iii) So we move on and choose another subgroup: $H = \{e, R_2\}$. In this case we leave you to check (see the next exercise) that all the left cosets are equal to the corresponding right cosets and that we get the following four cosets

$$\{e, R_2\}, \{R_1, R_3\}, \{S_1, S_2\}, \{S_3, S_4\}.$$

We give these cosets the labels H, H_1, H_2, H_3 respectively.

We now have to define the correct combination on the H's. This is done from the equation

$$f(g_1) \square f(g_2) = f(g_1 \circ g_2).$$

Remember that because of compatibility we can choose *any* g which maps to $f(g_1)$, etc. So, for instance, to find $H_2 \square H_3$ we choose any two g's which map to these H's.

$$S_1 \longmapsto H_2$$
$$S_3 \longmapsto H_3$$
$$S_1 \circ S_3 = R_1 \longmapsto H_1$$

so

$$H_2 \square H_3 = H_1.$$

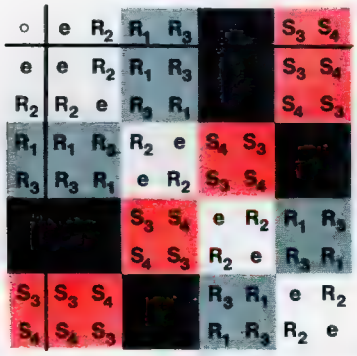
We ask you to show (in the next exercise) that the table for the H's is

$\square$	H	H_1	H_2	H_3
H	H	H_1	H_2	H_3
H_1	H_1	H	H_3	H_2
H_2	H_2	H_3	H	H_1
H_3	H_3	H_2	H_1	H

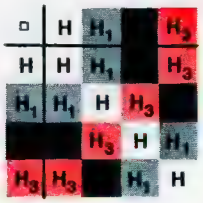
You may recognize this group as the Klein 4-group. The morphism f of $(G, \circ)$ to this group is defined by

$$f{:}e, R_2 \longmapsto H$$
$$f{:}R_1, R_3 \longmapsto H_1$$
$$f{:}S_1, S_2 \longmapsto H_2$$
$$f{:}S_3, S_4 \longmapsto H_3$$

We can see this very clearly if we rearrange the multiplication table of G in the following way:



The corresponding table for the cosets of H is



(iv) We ask you to consider the remaining subgroups in the next exercise. (We have effectively already considered $\{e, R_1, R_2, R_3\}$ in Exercise 33.1.2.4 (iii).) ■

Exercise 1

Exercise 1
(3 minutes)

We use the same notation as in Example 1.

$\circ$	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
e	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
R_1	R_1	R_2	R_3	e	S_4	S_3	S_1	S_2
R_2	R_2	R_3	e	R_1	S_2	S_1	S_4	S_3
R_3	R_3	e	R_1	R_2	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	e	R_2	R_1	R_3
S_2	S_2	S_4	S_1	S_3	R_2	e	R_3	R_1
S_3	S_3	S_2	S_4	S_1	R_3	R_1	e	R_2
S_4	S_4	S_1	S_3	S_2	R_1	R_3	R_2	e

(i) Show that $\{e, S_1\}$, $\{e, S_2\}$, $\{e, S_3\}$ cannot be the kernels of morphisms. (See Example 1, (ii).)

(ii) Show that for every choice of $g \in G$,

$$gH = Hg,$$

where $H = \{e, R_2\}$, and that the cosets of H are $\{e, R_2\}$, $\{R_1, R_3\}$, $\{S_1, S_2\}$, $\{S_3, S_4\}$. (See Example 1, (iii).)

(iii) Show that the combination table for the H's is as given in Example 1, (iii).

(iv) Consider the subgroup $H = \{e, R_1, R_2, R_3\}$. Show that

$$gH = Hg$$

for all $g \in G$. Hence find the cosets of H and construct the appropriate combination table for the cosets. (Compare your result with Exercise 33.1.2.4, (iii).)

(v) Repeat (iv) for the cases
(a) $H = \{e, R_2, S_1, S_2\}$,
(b) $H = \{e, R_2, S_3, S_4\}$. ■

We conclude this section with a few important notes:

Main Text
* * *

(i) If $(H, \circ)$ is a subgroup of $(G, \circ)$ for which

$$gH = Hg$$

for all $g \in G$, then H is called a normal subgroup of G.

Definition 1
* * *

(Other names used in the literature are *invariant* and *self-conjugate*.)

We can now state the main result of this section in the following way.

A subgroup $(H, \circ)$ of a group $(G, \circ)$ is the kernel of a morphism f from $(G, \circ)$ to a group $(f(G), \square)$ if and only if $(H, \circ)$ is a normal subgroup.

(ii) We have seen that, on the set of left (or right) cosets of a normal subgroup H, we can define a binary operation which turns the set of cosets into a group $(f(G), \square)$ which is a morphic image of $(G, \circ)$. This image group is called the factor group (or quotient group) of G modulo H and denoted by G/H.
The identity element of G/H is H.

Definition 2
* * *

(iii) Note that (ii) describes the situation when we do not have a morphism to start with, only the group $(G, \circ)$. Suppose on the other hand that we have a morphism

$$f: (G, \circ) \longmapsto (M, \square).$$

(continued on page 25)

Solution 1

(i) $R_1\{e, S_1\} = \{R_1, S_4\}$

$\{e, S_1\}R_1 = \{R_1, S_3\}$

so $\{e, S_1\}$ cannot be the kernel of a morphism. Similarly for the other two subgroups.

(iv) We can verify that $gH = Hg$ directly, or notice that

(a) we do not need to check for g equal to e, R_1, R_2, R_3;

(b) for g equal to S_1, S_2, S_3, S_4, $gH = Hg = \{S_1, S_2, S_3, S_4\}$ and so $gH = Hg$.

We get two cosets H and $H_1 = \{S_1, S_2, S_3, S_4\}$. The appropriate table is

$\square$	H	H_1
H	H	H_1
H_1	H_1	H

and the morphism of $(G, \circ)$ to this group is given by

$$e, R_1, R_2, R_3 \longmapsto H$$

$$S_1, S_2, S_3, S_4 \longmapsto H_1$$

The way in which this morphism acts on G is illustrated in the following diagrams.

$\circ$	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
e	e	R_1	R_2	R_3	S_1	S_2	S_3	S_4
R_1	R_1	R_2	R_3	e	S_4	S_3	S_1	S_2
R_2	R_2	R_3	e	R_1	S_2	S_1	S_4	S_3
R_3	R_3	e	R_1	R_2	S_3	S_4	S_2	S_1
S_1	S_1	S_3	S_2	S_4	e	R_2	R_1	R_3
S_2	S_2	S_4	S_1	S_3	R_2	e	R_3	R_1
S_3	S_3	S_2	S_4	S_1	R_3	R_1	e	R_2
S_4	S_4	S_1	S_3	S_2	R_1	R_3	R_2	e

$\square$	H	H_1
H	H	H_1
H_1	H_1	H

(v) (a) As in (iv), we have

$$gH = Hg \quad \text{for } g \in H,$$

and

$$gH = Hg = \{R_1, R_3, S_3, S_4\} = H_1 \quad \text{for } g \notin H,$$

so

$$\forall_g gH = Hg \qquad (g \in G).$$

The morphism is

$$e, R_2, S_1, S_2 \longmapsto H$$

$$R_1, R_3, S_3, S_4 \longmapsto H_1.$$

The table is the same as in (iv).

(b) Similarly, the morphism is

$$e, R_2, S_3, S_4 \longmapsto H$$

$$R_1, R_3, S_1, S_2 \longmapsto H_1,$$

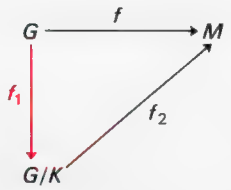
where

$$H_1 = \{R_1, R_3, S_1, S_2\}.$$

The table is the same as in (iv). ■

(*continued from page 23*)

Then f has a kernel K which is a normal subgroup of G. We can therefore form the factor group G/K of G modulo K. What is the connection between G/K and M? The elements of G/K are cosets and each coset corresponds to just one element of M. It is not difficult to see that G/K and M are isomorphic. We can illustrate this in a commutative diagram:



f is the given morphism with kernel K; f_1 is the morphism we have constructed (using K as the normal subgroup) and f_2 is the isomorphism which links G/K and M.

$$f = f_2 \circ f_1.$$

This link between the construction of a morphism f_1 and an existing morphism f is discussed in the television programme associated with this unit.

(iv) In the text we have chosen labels for the cosets. In the literature it is usual in theoretical work to use the labels we used originally, e.g. gK. If $g_1 \in gK$ then

$$g_1K = gK$$

and so g_1K is also a label for the same coset. This notation has the disadvantage that each coset has several labels, but it does, however, have the advantage of giving an easily remembered form for $\square$:

$$gK \,\square\, g_1K = (g \circ g_1)K.$$

(v) In an Abelian (commutative) group, every subgroup $(K, \circ)$ is normal, since

$$\begin{aligned} g_1K &= \{g : g = g_1 \circ k, k \in K\} \\ &= \{g : g = k \circ g_1, k \in K\} \\ &= Kg_1 \quad \text{for all } g_1 \in G. \end{aligned}$$

(vi) Even if a group $(G, \circ)$ is not commutative, there is always a non-empty subset Z_G of G such that any element of Z_G commutes with *every* element of G.

Z_G is called the centre of $(G, \circ)$; **Definition 3** * *

$$Z_G = \{z : z \in G, z \circ g = g \circ z, g \in G\}.$$

(vii) If $(H, \circ)$ is a subgroup of $(G, \circ)$ and G is the union of just *two* cosets of H, then we must have

$$G = H \cup gH = H \cup Hg \qquad g \notin H.$$

(This is because the cosets H and gH have no common elements. We prove this on page 29.) Hence

$$gH = Hg \qquad g \notin H.$$

We know that

$$gH = Hg \qquad g \in H,$$

so $(H, \circ)$ is a normal subgroup. (Have another look at the subgroups of order four in Example 1.)

Exercise 2

Exercise 2
(4 minutes)

Consider the group with table

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Consider the four subgroups: $\{e, a, b\}$, $\{e, c\}$, $\{e, d\}$, $\{e, f\}$. Are any of them normal subgroups? For any subgroup which is a normal subgroup, find the factor group and write down its group table. ■

Exercise 3

Exercise 3
(5 minutes)

(i) How do we know that the centre of a group is not empty?
(ii) Prove that $(Z_G, \circ)$ is a subgroup of $(G, \circ)$.
(iii) Prove that $(Z_G, \circ)$ is a normal subgroup.
(iv) Find the centre of the symmetry group of the square. ■

We conclude this section with two examples which concern groups we have met elsewhere in the course.

Example 2

Example 2

Let $(G, \circ)$ be the group of integers under addition. The group is commutative and so every subgroup is a normal subgroup. For example, consider the subgroup S of integers which are multiples of 5.

$$S = \{\ldots -15, -10, -5, 0, 5, 10, \ldots\}.$$

The cosets of S are

S itself

$$\{\ldots, -9, -4, 1, 6, 11, \ldots\} = A$$

$$\{\ldots, -8, -3, 2, 7, 12, \ldots\} = B$$

$$\{\ldots, -7, -2, 3, 8, 13, \ldots\} = C$$

$$\{\ldots, -6, -1, 4, 9, 14, \ldots\} = D$$

The factor group G/S is the group of these 5 equivalence classes under the "addition" operation induced on them. It has the following group table:

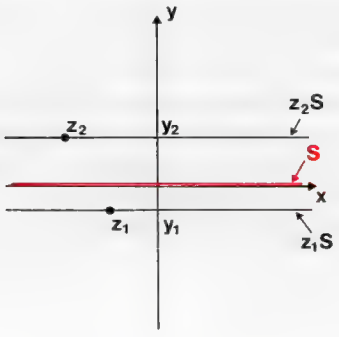
□	S	A	B	C	D
S	S	A	B	C	D
A	A	B	C	D	S
B	B	C	D	S	A
C	C	D	S	A	B
D	D	S	A	B	C

$(G/S, \square)$ is isomorphic to the group $\{0, 1, 2, 3, 4\}$ with the operation $\oplus_5$. ■

Example 3

Example 3

Let $(G, \circ)$ be the group of complex numbers under addition. Again, the group is commutative and so every subgroup is a normal subgroup. Consider the subgroup, $S = \{x + 0i : x \in R\}$, of complex numbers with imaginary part zero. S can be illustrated on an Argand diagram:



The cosets are formed by taking an arbitrary complex number and combining it in turn with each element of S. They correspond in the Argand diagram to straight lines parallel to the x-axis. (The distinguishing feature of any coset is that every element in it has the same imaginary part.) The factor group G/S forms a group for the induced "addition" operation, by which a coset corresponding to the complex number z_1 (with imaginary part y_1) "added" to a coset corresponding to z_2 (with imaginary part y_2) gives the coset corresponding to $z_1 + z_2$ (with imaginary part $y_1 + y_2$). It is clear that each coset can be represented by an imaginary part and that the mapping $(G/S, \square) \longmapsto (R, +)$ is an isomorphism. ■

We have seen then, that assuming we can list all the subgroups of a group G, we can test them for normality and predict precisely what groups can arise as homomorphic images of the given group G. Any such group *must* be isomorphic to G/S where S is some normal subgroup of G. Once we have found all the normal subgroups of G we know exactly what form any homomorphic image of G will take.

Discussion
* *

Solution 2

Solution 2

Only the subgroup $\{e, a, b\}$ is normal. The cosets are $\{e, a, b\}$, $\{c, d, f\}$.

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

Labelling these 0 and 1 respectively, the factor group has the table:

$\square$	0	1
0	0	1
1	1	0

— it is the group which we met on pages 3 and 24. ■

Solution 3

Solution 3

(i) $e \in Z_G$, since $e \circ g = g \circ e = g$ for all $g \in G$.

(ii) We know that $e \in Z_G$ and that $\circ$ is associative; so we have to prove that Z_G is closed and contains inverses.

Closure

Suppose $z_1, z_2 \in Z_G$, then

$$\left.\begin{aligned} z_1 \circ g &= g \circ z_1 \\ z_2 \circ g &= g \circ z_2 \end{aligned}\right\} g \in G$$

We wish to show that $z_1 \circ z_2 \in Z_G$. Now

$$\begin{aligned} (z_1 \circ z_2) \circ g &= z_1 \circ (z_2 \circ g) = z_1 \circ (g \circ z_2) \\ &= (z_1 \circ g) \circ z_2 = (g \circ z_1) \circ z_2 \\ &= g \circ (z_1 \circ z_2), \end{aligned}$$

so $z_1 \circ z_2$ commutes with all elements of G, i.e. $z_1 \circ z_2 \in Z_G$.

Inverses

If $z_1 \in Z_G$, then

$$z_1 \circ g = g \circ z_1$$

i.e.

$$z_1^{-1} \circ (z_1 \circ g) = z_1^{-1} \circ (g \circ z_1)$$

i.e.

$$g = z_1^{-1} \circ g \circ z_1$$

whence

$$\begin{aligned} g \circ z_1^{-1} &= (z_1^{-1} \circ g \circ z_1) \circ z_1^{-1} \\ &= z_1^{-1} \circ g \end{aligned}$$

so

$$z_1^{-1} \in Z_G.$$

So $(Z_G, \circ)$ is a subgroup of $(G, \circ)$.

(iii) The fact that $(Z_G, \circ)$ is normal is clear from the fact that the elements of Z_G commute with every element of G.

(iv) $Z_G = \{e, R_2\}$. (See the table on page 24.) ■

33.1.4 Looking for Subgroups of a Finite Group

33.1.4

Discussion

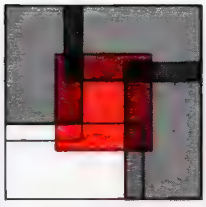
* *

An immediate consequence of our discussion in the last section is that we have a method of finding all the homomorphisms from a given group $(G, \circ)$. All we need to do is to find all the subgroups of $(G, \circ)$ and test each of them to see if it is a normal subgroup. But that is not as easy as it sounds. For example, suppose we take a group containing nine elements. On the face of it we have to take every subset and test to see if it gives a subgroup, and then take all the subgroups we have found and test to see which ones are normal subgroups. And there are $2^9 = 512$ subsets! (Admittedly, we know that we must include the identity element in any subgroup — but that still leaves $2^8 = 256$ subsets to try.) Fortunately, there is a theorem which comes to the rescue which immediately limits the number of subsets which we need to consider. The theorem also has many interesting and important theoretical consequences. *It applies only to groups with a finite number of elements.*

We have all the technique required to prove this theorem at hand; in our desire to investigate the factor group we have overlooked some useful facts.

One thing which you may have noticed when forming cosets of a subgroup is that each of the cosets contains the *same number of elements*, and this is the same as the *number of elements in the subgroup.* This is in fact always the case whether or not the subgroup is normal, and we can show this as follows.

Any coset gS of a subgroup S is formed by combining g with each element of S in turn. Each of these combinations is different from the others, because if $g \circ s_1 = g \circ s_2$ then it follows that $s_1 = s_2$. Thus as we run through all the elements of S we generate one new element for each element of S: gS contains the same number of elements as S. (Remember that S contains a finite number of elements.) Since $e \in S$, $g \circ e \in gS$, so every element of G belongs to some coset. So the cosets are a set of subsets which cover (i.e. whose union is) G. At first we might suppose that the cosets cover G in the following way:



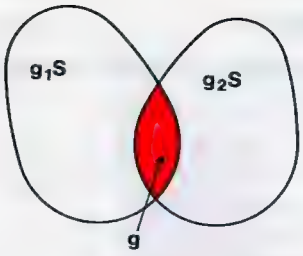
i.e. the cosets overlap. But none of the examples we have seen has given overlapping cosets: we had either

$$g_1S = g_2S$$

or

$$g_1S \cap g_2S = \varnothing.$$

We shall now prove that cosets do not overlap.
Suppose we form a coset g_2S and then pick an element g_1 not in g_2S and form the coset g_1S. Suppose further (contrary to what we want to prove) that the two cosets g_1S and g_2S overlap. (We are dealing here with left cosets — a similar argument can be used for right cosets.)



Then there is an element, g, belonging to both g_1S and g_2S. Thus we can find elements s_1 and s_2 in the subgroup S such that

$$g = g_1 \circ s_1$$

and

$$g = g_2 \circ s_2.$$

That is to say

$$g_1 \circ s_1 = g_2 \circ s_2,$$

and since S is a subgroup, the inverse of s_1 is in S, so we have

$$g_1 \circ s_1 \circ s_1^{-1} = g_2 \circ s_2 \circ s_1^{-1}.$$

We can put $s_2 \circ s_1^{-1} = s_3$, where $s_3 \in S$, since $(S, \circ)$ is a group, giving

$$g_1 = g_2 \circ s_3,$$

and thus g_1 belongs to g_2S, which contradicts our original assumption. Thus if we start with an element g_1 *not* in g_2S we generate *a completely distinct* coset g_1S, that is,

$$g_1S \cap g_2S = \varnothing.$$

What happens if we start with an element g_1 which *is* in g_2S? In that case there is an element s_4 in S which is such that

$$g_1 = g_2 \circ s_4.$$

Any element of g_1S is of the form $g_1 \circ s$ for some $s \in S$ and

$$g_1 \circ s = g_2 \circ s_4 \circ s,$$

and since S is a subgroup, $s_4 \circ s$ is an element of S, say s_5. Thus

$$g_1 \circ s = g_2 \circ s_5,$$

showing that $g_1 \circ s$ belongs to g_2S. Thus, whatever element of S we combine with g_1, we stay inside g_2S.

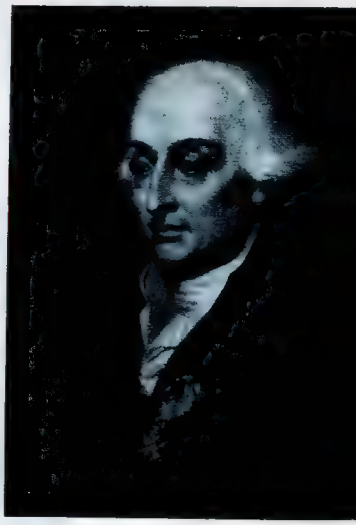
We have shown therefore that any two cosets of S in G are either distinct (with no element in common) or identical.

Now suppose S contains x elements and suppose S gives us y distinct cosets. Then since these cosets *are* distinct and because they together give us all the elements of the complete group, the product xy is exactly the number of elements in the group. So if the group contains n elements (i.e. the group has order n), then $n = xy$, or $\frac{n}{x} = y$, where y is an integer. This is

LAGRANGE'S THEOREM:

The order of a subgroup is a factor of the order of the group.

Thus, for example, we know that in a group of order 9 a subgroup must have either 1 or 3 or 9 elements. There is only one subgroup with 1 element — the trivial subgroup $\{e\}$. There is only one subgroup with 9 elements —



Joseph-Louis Lagrange
1736–1813
(Mansell Collection)

the group itself. Any other subgroup must contain three elements. One of these must be the identity element: the other two elements can be chosen in 28 ways, each of which would have to be investigated.

Exercise 1

Exercise 1
(3 minutes)

(i) A group $(G, \circ)$ has order p, where p is a prime. Describe the possible morphisms of G.

(ii) If f is a morphism from a (finite) group $(G, \circ)$ to a group $(H, \square)$, show that the number of elements in H is a factor of the number of elements in G. ■

Exercise 2

Exercise 2
(4 minutes)

Let $(G, \circ)$ be a group of order n. We denote by g^t the element of G obtained by combining g with itself:

$$\underbrace{g \circ g \circ g \circ g \circ \ldots \circ g}_{(t \text{ terms})}.$$

(i) Show that for some r, $g^r = e$.

(ii) If h is the smallest natural number for which $g^h = e$, show that the subset

$$\{g, g^2, g^3, \ldots, g^h = e\}$$

is a subgroup of G.
Hence deduce that h is a factor of the order of the group, n.

(iii) If n is a prime number, deduce that all groups of order n are isomorphic.

■

Solution 1

Solution 1

(i) Lagrange's theorem tells us that, since the order of the group is prime, the group has no subgroups besides the group itself and the identity element. Although these can both be considered as normal subgroups, they are only such in a trivial sense.

The cosets formed by $\{e\}$ are just the single elements of the group and the factor group $G/\{e\}$ is isomorphic to the group itself.

Considered as a normal subgroup, the group itself has just one coset — itself; the factor group G/G contains just one element. (Again, we are not making a distinction between a set with only one element and the element itself.)

(ii) If G has order n and the kernel of the morphism has order k, then there are n/k cosets and so H has order n/k, a factor of n. ■

Solution 2

Solution 2

(i) Since the group is finite, not all

$$g^t \qquad t = 1, 2, 3, \ldots$$

can be different. Suppose

$$g^t = g^s, \quad \text{where } s > t,$$

then by using g^{-1} t times on each side, we get

$$e = g^{s-t}, \quad \text{so } r = s - t.$$

(ii) We have to show that the set is closed and contains its inverses.

Closure

$$g^r \circ g^s = g^{r+s} \qquad r < h \quad \text{and} \quad s < h.$$

Now either $r + s \leqslant h$, in which case it is obviously an element of the subset, or $r + s > h$, in which case

$$\begin{aligned} g^{r+s} &= g^{r+s-h}g^h \\ &= g^{r+s-h}, \qquad \text{since } g^h = e, \end{aligned}$$

which again is an element of the subset.

Inverses

The inverse of g^r $(r < h)$ is g^{h-r}. Hence the subset is a group. It contains h elements, so by Lagrange's theorem, h divides n.

(iii) Consider any element g $(\neq e)$ of the group. The elements

$$g, g^2, g^3, \ldots, g^N = e$$

form a subgroup. This subgroup cannot contain fewer than n elements, because if it contained $h < n$ elements, h would have to divide n, which it cannot, because n is prime, so $N = n$. So the whole group can be generated from any one of its elements (except the identity). Any other group of order n will be of the same form: i.e. if r $(\neq e)$ is any element, the group is

$$\{r, r^2, r^3, \ldots, r^n = e\},$$

and the mapping $g \longmapsto r$ is an isomorphism. Remembering that in *Unit 30, Groups I*, we defined a cyclic group as a group generated by just one element, we see that if n is prime, the only group of order n is the cyclic group C_n.

We can thus assert with full confidence, that there is essentially only one group of order 53, for instance. Some very simple results in group

theory are beginning to pay off with some very general results: instead of having to consider 2^{52} subsets of a group of order 53 to determine all the subgroups, we can deal with the problem in one line. ■

33.2 CONCLUSION

33.2

Conclusion
* *

In these two units on groups we have established three results which are very important in group theory, in the sense that they provide a platform on which we can develop a systematic treatment of the subject. Our purpose was to find out what groups are, the sort of mathematics which is involved in group theory, and to glimpse some of the many beautiful ideas which follow from the four group axioms. We have had a glimpse at the power of such results: Cayley's theorem telling us that *any* group can be looked on as a subgroup of a group of permutations; Lagrange's theorem telling us something about *every* subgroup of any given finite group, and the far-reaching consequences which follow immediately; and the idea of a factor group telling us how to construct *every* homomorphic image of a group.

Unit No.	Title of Text
1	Functions
2	Errors and Accuracy
3	Operations and Morphisms
4	Finite Differences
5	NO TEXT
6	Inequalities
7	Sequences and Limits I
8	Computing I
9	Integration I
10	NO TEXT
11	Logic I — Boolean Algebra
12	Differentiation I
13	Integration II
14	Sequences and Limits II
15	Differentiation II
16	Probability and Statistics I
17	Logic II — Proof
18	Probability and Statistics II
19	Relations
20	Computing II
21	Probability and Statistics III
22	Linear Algebra I
23	Linear Algebra II
24	Differential Equations I
25	NO TEXT
26	Linear Algebra III
27	Complex Numbers I
28	Linear Algebra IV
29	Complex Numbers II
30	Groups I
31	Differential Equations II
32	NO TEXT
33	Groups II
34	Number Systems
35	Topology
36	Mathematical Structures